

## REMARKS

By this Amendment, claims 1-24 are amended, and claims 29-32 are added. Claims 25-28 remain in the application. Thus, claims 1-32 are active in the application. Reexamination and reconsideration of the application are respectfully requested.

In item 3 on page 2 of the Office Action, claims 1-4, 6-9, 11-14 and 16-19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Palage et al. (U.S. 6,247,133) in view of Katz et al. (U.S. 5,926,624) and further in view of Yahoo! Media Relations "Yahoo Mail Introduces New Virus Scan Feature" (Yahoo).

Without intending to acquiesce to this rejection, claims 1-2, 6-7, 11-12 and 16-17 have each been amended in order to more clearly illustrate the marked differences between the present invention and the applied references. Accordingly, the Applicants respectfully submit that the present application is clearly patentable over the applied references for the following reasons.

In conventional systems and methods, as described in the Description of the Background Art section of the specification, an information user of the data terminal equipment cannot authorize the authenticity of content data received from a server until after the information user has actually received the content data from the server. Accordingly, in the conventional systems and methods, once a user has received unauthentic content data, the information user either has wasted his or her time acquiring the unauthorized content data, or the information user may become a victim of so-called cracking, where, for example, the information user's personal information may be stolen.

Furthermore, in the conventional systems and methods, the information user must access a third-party authorization agency, which authorizes whether the content data stored on the server is authentic, in order to determine whether or not any received content data is authentic.

Accordingly, an object of the present invention is to provide a user data terminal equipment which is capable of authenticating content data before actually retrieving the content data from a server. Another object of the present invention is to provide a user data terminal equipment which is capable of authenticating content data without accessing a third-party authorization agency.

To achieve these objects, the data terminal equipment of the present invention, as well as the method performed by the data terminal equipment, determines the authenticity of a content data prior to retrieving the content data from the server. Furthermore, the data terminal equipment confirms the authenticity of the content data by using a retrieved index data indicating the content data and do not require accessing external servers or information sources to authenticate. Thus, the data terminal equipment of the present invention performs a unique effect in that traffic over a network is reduced.

The data terminal equipment of the present invention comprises an index retrieval part and an authentication part.

The index retrieval part retrieves index data indicating a content data prior to retrieving the content data. The index data includes embedded data which has been embedded with a locator (a locator which has been assigned to the content data) as an electronic watermark by an authorization agency. The index data can also include a location to which the content data is linked. When the index retrieval part has retrieved the index data, the embedded data having the locator is held in the data terminal equipment. If the index data includes the location, the location is also held in the data terminal equipment.

The authentication part authenticates the content data by using the index data (i.e., the index data which is held in the in the data terminal equipment). More specifically, the authentication part extracts the locator from the embedded data included in the retrieved index data, and confirms the authenticity of the content data if the locator is successfully extracted. Alternatively, the authentication part confirms the authenticity of the content data if the watermark locator is successfully extracted, and the extracted locator matches with the location that is included in the retrieved index data.

Accordingly, the data terminal equipment of the present invention retrieves the embedded data (the index data) prior to retrieving the content data, and internally confirms the authenticity of the content data without accessing an external server for authentication of the content data.

Independent claims 1-2, 6-7, 11-12 and 16-17 recite the above-described features of the present invention.

In particular, claim 1 recites the data terminal equipment as comprising an index retrieval part operable to retrieve index data indicating the content data prior to retrieving the content data, and an authentication part operable to authenticate the content by using the index data retrieved by the index retrieval part. Claim 1 also defines that the content data is assigned a locator indicating information for specifying a storage location thereof, and that the index data includes embedded data in which the locator is embedded as an electronic watermark by an authorization agency. Furthermore, claim 1 recites that the authentication part is operable to extract the locator from the embedded data included in the index data retrieved by the index retrieval part, and to confirm the authenticity of the content data if the locator is successfully extracted.

Claims 6, 11 and 16 recite a method as comprising retrieving index data indicating the content data prior to retrieving the content data, and authenticating the content data by using the index data retrieved in the retrieving. Claims 6, 11 and 16 also define that the content data is assigned a locator indicating information for specifying a storage location thereof, and that the index data includes embedded data in which the locator is embedded as an electronic watermark by an authorization agency. Furthermore, claims 6, 11 and 16 recite that the authenticating operation further comprises extracting the watermark locator from the embedded data included in the index data retrieved in the retrieving, and confirming the authenticity of the content data if the watermark locator is successfully extracted in the extracting.

Claim 2 recites the data terminal equipment as comprising an index retrieval part operable to retrieve index data indicating the content data prior to retrieving the content data, and an authentication part operable to authenticate the content data by using the index data retrieved by the index retrieval part. Claim 2 defines that the content data is assigned a locator indicating information for specifying a storage location thereof, and that the index data includes embedded data which is embedded with the locator as an electronic watermark by an authorization agency, and a location to which the content data is linked. Furthermore, claim 2 recites that the authentication part is operable to extract the locator from the embedded data included in the index data retrieved by the index retrieval part, and to confirm the authenticity of the content data if the watermark locator

is successfully extracted and the extracted locator matches with the location included in the index data retrieved by the index retrieval part.

Claims 7, 12 and 17 recite a method as comprising retrieving index data indicating the content data prior to retrieving the content data, and authenticating the content data by using the index data retrieved in the retrieving. Claims 7, 12 and 17 also define that the content data is assigned a locator indicating information for specifying a storage location thereof, and that the index data includes embedded data which is embedded with the locator as an electronic watermark by an authorization agency, and a location to which the content data is linked. Furthermore, claims 7, 12 and 17 recite the authenticating operation as further comprising: extracting, as a watermark locator, the locator embedded as the electronic watermark from the embedded data included in the index data retrieved in the retrieving; extracting, as a text locator, the location from the index data retrieved in the retrieving if the watermark locator has been successfully extracted in the watermark locator extracting; determining whether the text locator extracted in the text locator extracting matches with the watermark locator extracted in the watermark locator extracting; and confirming the authenticity of the content data only if it is determined in the determining that the text locator matches with the watermark locator.

In item 4 on pages 2-3 of the Office Action, the Examiner contends that Palage et al. discloses the index retrieval part of claims 1 and 2. Despite the Examiner's assertion to the contrary, Palage et al. does not disclose or suggest retrieve index data indicating the content data prior to retrieving the content data. As is evident from Column 5, lines 30-47 of Palage et al., Palage et al. discloses that a document identifier, such as an image file and hypertext link, are contained in an electronic document to be authenticated. Accordingly, the document viewer 1 of Palage et al. must therefore obtain a HTML text file (i.e., a content data) in its entirety in order to retrieve the document identifier (i.e., the image file and hypertext link).

Therefore, Palage et al. discloses receiving the document identifier together with the content data. Accordingly, Palage et al. clearly does not disclose or suggest an index retrieval part operable to retrieve index data indicating the content data prior to retrieving

the content data, as recited in claims 1 and 2, and retrieving index data indicating the content data prior to retrieving the content data, as recited in claims 6-7, 11-12 and 16-17.

The Examiner also alleges that Palage et al. discloses the authentication part of claims 1 and 2. However, despite the Examiner's assertion to the contrary, Palage et al. fails to disclose or suggest an authentication part comprised in the document viewer 1 that confirms the authenticity of the content data. In particular, as described in Column 6, lines 50-57, Palage et al. discloses that a verification server 6 accesses a data server based on the document identifier that is contained in a verification signal from the document viewer 1. That is, the document viewer 1 retrieves the document identifier together with the content data and sends the retrieved document identifier to the verification server 6 without confirming the authenticity of the content data. Instead of the document viewer 1 performing the authentication of the content data, the verification server 6, which is external to the document viewer 1, authenticates the content data by using the document identifier sent from the document viewer 1.

Accordingly, Palage et al. clearly does not disclose or suggest an authentication part operable to extract the locator from the embedded data included in the index data retrieved by the index retrieval part, and to confirm the authenticity of the of the content data if the locator is successfully extracted, as recited in claim 1. Similarly, Palage et al. also clearly fails to disclose or suggest extracting the watermark locator from the embedded data included in the index data retrieved in the retrieving, and confirming the authenticity of the content data if the watermark locator is successfully extracted in the extracting, as recited in claims 6, 11 and 16.

Moreover, for the foregoing reasons, Palage et al. clearly fails to disclose an authentication part operable to extract the locator from the embedded data included in the index data retrieved by the index retrieval part, and to confirm the authenticity of the content data if the watermark locator is successfully extracted and the extracted locator matches with the location included in the index data retrieved by the index retrieval part, as recited in claim 2. Similarly, Palage et al. also clearly fails to disclose or suggest extracting, as a watermark locator, the locator embedded as the electronic watermark from the embedded data included in the index data retrieved in the retrieving; extracting, as a text locator, the location from the index data retrieved in the retrieving if the

watermark locator has been successfully extracted in the watermark locator extracting; determining whether the text locator extracted in the text locator extracting matches with the watermark locator extracted in the watermark locator extracting; and confirming the authenticity of the content data only if it is determined in the determining that the text locator matches with the watermark locator, as recited in claims 7, 12 and 17.

Similar to Palage et al., Katz et al. also fails to disclose or suggest that index data indicating content data is retrieved prior to the content data, where the content data is assigned a locator indicating information for specifying a storage location thereof, and the index data includes embedded data in which the locator is embedded as an electronic watermark by an authorization agency. Instead, Katz et al. merely discloses that a client browser 219 executing on a client computer system 214 can make requests for library data from a library sever 260 (see Column 8, line 63 to Column 9, line 6).

Accordingly, similar to Palage et al., Katz et al. clearly does not disclose or suggest retrieving index data indicating the data blocks prior to receiving the data blocks, where the content data is assigned a locator indicating information for specifying a storage location thereof, and the index data includes embedded data in which the locator is embedded as an electronic watermark by an authorization agency, as recited in claims 1-2, 6-7 and 11-12 and 16-17.

Moreover, Katz et al. also clearly fails to disclose or suggest the authenticity confirmation operations of claims 1-2, 6-7 and 11-12 and 16-17.

Furthermore, Yahoo also clearly does not disclose or suggest retrieving index data indicating the content data prior to retrieving the content data, and the authenticity confirmation operations of claims 1-2, 6-7 and 11-12 and 16-17.

Therefore, no obvious combination of Palage et al., Katz et al. and Yahoo would result in the inventions of claims 1-2, 6-7 and 11-12 and 16-17 since Palage et al., Katz et al. and Yahoo, either individually or in combination, clearly fail to disclose or suggest each and every limitation of claims 1-2, 6-7 and 11-12 and 16-17.

Accordingly, claims 1-2, 6-7 and 11-12 and 16-17 are clearly patentable over Palage et al., Katz et al. and Yahoo since Palage et al., Katz et al. and Yahoo, either individually or in combination, clearly fail to disclose or suggest each and every limitation of claims 1-2, 6-7 and 11-12 and 16-17.

In item 7 on page 4 of the Office Action, claims 5, 10, 15 and 20-24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Palage et al. in view of Katz et al. and Yahoo and further in view of Moskowitz et al. (U.S. 5,905,800). Further, in item 9 on page 5 of the Office Action, claims 25-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Palage et al. in view of Katz et al. and Yahoo and further in view of Klug (U.S. 6,591,245).

As demonstrated above, Palage et al., Klatz et al. and Yahoo do not disclose or suggest each and every limitation of claims 1-2, 6-7 and 11-12 and 16-17. Similarly, Moskowitz et al. and Klug also do not disclose or suggest retrieving index data indicating the content data prior to retrieving the content data, and the authenticity confirmation operations of claims 1-2, 6-7 and 11-12 and 16-17.

Therefore, Moskowitz et al. and Klug do not cure the deficiencies of Palage et al., Klatz et al. and Yahoo for failing to disclose or suggest each and every limitation of claims 1-2, 6-7 and 11-12 and 16-17.

Furthermore, Palage et al., Klatz et al., Yahoo, Moskowitz et al. and Klug, either individually or in combination, do not disclose or suggest the effects achieved by the inventions of claims 1-2, 6-7 and 11-12 and 16-17. As mentioned above, the present invention retrieves the embedded data (the index data) prior to retrieving the content data, and internally confirms the authenticity of the content data without accessing an external server for authentication of the content data.

However, Palage et al., Klatz et al., Yahoo, Moskowitz et al. and Klug do not even contemplate authenticating content data without accessing an external server or data source for authentication. Therefore, one skilled in the art would not arrive at the inventions of claims 1-2, 6-7 and 11-12 and 16-17 by any combination of Palage et al., Klatz et al., Yahoo, Moskowitz et al. and Klug since these references, either individually or in combination, do not disclose or suggest each and every limitation of claims 1-2, 6-7 and 11-12 and 16-17, and do not even contemplate achieving the effects of the inventions of claims 1-2, 6-7 and 11-12 and 16-17.

Because of the clear distinctions discussed above, it is submitted that the teachings of Palage et al., Klatz et al., Yahoo, Moskowitz et al. and Klug clearly do not meet each and every limitation of claims 1-2, 6-7 and 11-12 and 16-17.

Furthermore, it is submitted that the distinctions discussed above are such that a person having ordinary skill in the art at the time the invention was made would not have been motivated to modify Palage et al., Klatz et al., Yahoo, Moskowitz et al. and Klug in such a manner as to result in, or otherwise render obvious, the present invention as recited in claims 1-2, 6-7 and 11-12 and 16-17.

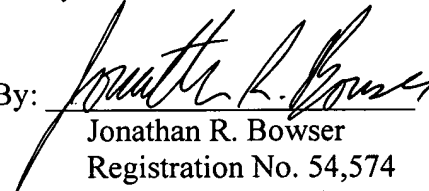
Therefore, it is submitted that the claims 1-2, 6-7 and 11-12 and 16-17, as well as claims 3-5, 8-10, 13-15 and 18-32 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

Masayuki KUMAZAWA et al.

By:   
Jonathan R. Bowser  
Registration No. 54,574  
Attorney for Applicants

JRB/nrj  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
December 7, 2005